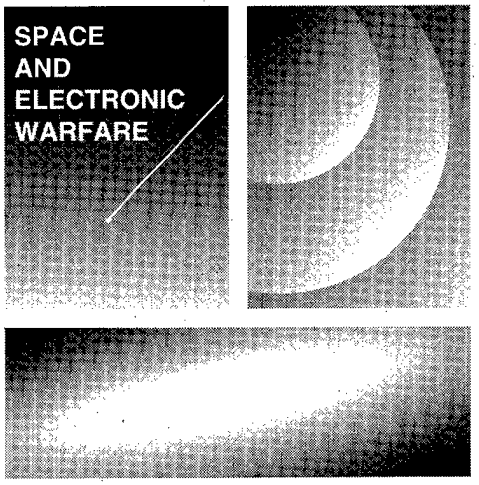


Accession Number: 3614

Publication Date: Jun 01, 1992

Title: Space and Electronic Warfare, A Navy Policy Paper on a New Warfare Area

Personal Author: Loescher, M.S.

Corporate Author Or Publisher: Director, Space & Electronic Warfare(OP-094), OCNO, The Pentagon, Wash

Comments on Document: Second paper in a trilogy

Descriptors, Keywords: Space Electronic Warfare SEW Copernicus Croesus Sonata C4I Battle Space Modeling Commander Surveillance Communication Grid

Pages: 00026

Cataloged Date: Jul 09, 1992

Document Type: HC

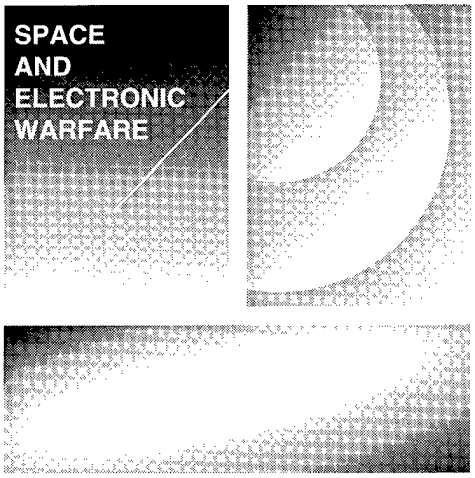
Number of Copies In Library: 000002

Record ID: 24277

SPACE AND ELECTRONIC WARFARE

A Navy Policy Paper on a New Warfare Area

JUNE 1992



Director, Space and Electronic Warfare (OP-094)
Office of the Chief of Naval Operations
Room 5B740, The Pentagon
Washington, D.C. 20301

TABLE OF CONTENTS

LIST OF FIGURES

"In the land of the blind, the one-eyed man is king"
Erasmus

INTRODUCTION

We live in a new world. Yet, even in such a world there are constants. We are inextricably tied to our geography; ours will remain a maritime nation in need of a strong navy. Nonetheless, navies are effective only insofar as they are able to influence events ashore—their value is affected by their ability to project power and keep pace with changes in the nature of land warfare.

While war at sea has typically been quick, violent, decisive, capital-intensive, and rare; war ashore among industrialized nations has taken on those characteristics only recently. Both forms of warfare are now dominated by speed, surveillance, command and control, and the importance of firing effectively first.

Increasingly, the object of a land campaign is not the territory on which it is fought, but the destruction of certain capital assets to deny the enemy's strategic choices. In this form of warfare the enemy's strategic center of gravity will include the enemy decision-maker, his command and control, and his surveillance systems.

As a matter of policy, industrialized nations use technology to facilitate the substitution of capital for labor in warfighting. That is, the policy is to shoot more and fight less. Technological development and insertion has increased the rate of substitution dramatically. Electronics technologies in particular are responsible for the revolution in warfare. They appear in precision guided weapons, integrated surveillance systems including space-based systems, high-speed decision aids, netted command and control systems, and increasingly sophisticated command and control, communications, and electronic combat systems. Once considered visionary, such capabilities are now reality.

As a result, a relatively few important capital targets can be destroyed quickly with profound effect—and a new warfare area, Space and Electronic Warfare (SEW), has emerged.

SPACE AND ELECTRONIC WARFARE

In 1989, the Chief of Naval Operations formally designated SEW as a Navy warfare mission area. All principal warfare mission areas have two unique features:

- First, they have a strategic objective, one which significantly influences the scope, pace, or intensity of conflict, and;
- Second, they have a clearly defined target set.

The *strategic objective* of SEW is to separate the enemy from his forces, to render the leader remote from his people (to take command of his forces in effect), and control his use of the electromagnetic spectra. This objective dominates when our quarrel is not with the people but with the enemy leadership, when it is highly desirable to limit damage, contain the conflict, and terminate quickly. The despotic regimes likely to be our adversaries are characterized by centralized leadership; hierarchical command and control structures; and control of the press and information infrastructure. In the face of new technologies, these features—however modern and redundant—are vulnerable.

The *target set* consists of those systems, which when destroyed, yield the strategic objective. For SEW, the target set consists of the enemy leadership at all levels including the battlefield level, its communications systems, surveillance and targeting systems, information processing, decision and

display systems, electronic warfare systems, and weapons guidance systems. An attack on this target set is the epitome of power projection, the ultimate penetration of the enemy. Naval forces operating in conjunction with other U.S. and allied forces will play a critical role. These are the operations that enable "maneuver warfare."

At the same time, the technological revolution, especially in information management, is presenting still other opportunities—for friend and foe alike. The advent of the modern computer workstation, the on-going development of a global, commercial communications infrastructure, and the proliferation of "smart" weapons throughout the militarized world, all of which can be bought "off-the-shelf," have the potential to make a weak foe strong in a very short time. These developments paradoxically could provide a significant advantage to a small, wealthy regime and disadvantages to western militaries unless our acquisition of systems is streamlined to capture commercial innovation.

We may conclude that just as the hostile SEW target set presents an opportunity for us, so does it also for potential foes. Indeed, for a small country seeking the tactical center of gravity of an overwhelming force, the SEW assets of the latter will be an irresistible target. We must develop a SEW-protect capability. While Desert Storm appeared to the public to be a high technology war in all aspects, many systems were several generations behind available commercial technology and were, in fact, vulnerable.

SEW DEFINED

We conduct SEW, then, both in terms of *warfare* and *warfare support* functions. Formally defined, SEW is the destruction or neutralization of enemy SEW targets. As warfare support, it is the enhancement of friendly force battle management through the integrated employment and exploitation of the electromagnetic spectra and the medium of space. It encompasses measures that are employed to:

- Coordinate, correlate, fuse, and employ active and passive systems to optimize individual and aggregate communication, surveillance, reconnaissance, data correlation, classification, targeting and electromagnetic attack capabilities;

- Destroy, deny, degrade, confuse, or deceive the enemy's capabilities to communicate, sense, reconnoiter, classify, target, and direct an attack; and,

- Direct and control the employment of friendly forces and the information necessary to provide for the administration and support of those forces.

Such definitions require operational context.

Establishing SEW as a warfare mission area reflects recognition that *information* is the key to the hostile decision-making process, whatever it is and whatever form it might be. In that sense, SEW incorporates information warfare.

It also implies the technological maturity to operate in and against the fourth and fifth dimensions of battle space: the geography of space and the physics of the electromagnetic spectra. In this sense, the advent of SEW has clear parallels with the development of other naval warfare areas.

Since World War I, military doctrine has been centered on maneuver warfare—the avoidance of the horrible and costly stalemate of the trenches. Armored warfare, airborne assault, blitzkrieg, amphibious assault, strategic bombing: all these are aimed at maneuver—breaking out, preventing static tactical dilemmas.

Naval warfare has proceeded somewhat differently; its impetus has been technology. Surface warfare, for 3,000 years the naval paradigm, was expanded to include subsurface warfare with the advent of the submarine. Anti-submarine warfare, defined by the target set of the submarine,

Navy SEW Policy

- The strategic objective of SEW is to separate the enemy leader from his forces, to render him remote from his people (to take command of his forces in effect), and to control his use of the electromagnetic spectra.

- The SEW target set consists of those systems, which when destroyed, yield the strategic objective. The set includes the enemy leadership at all levels including the battle field level, its communications systems, surveillance and targeting systems, information processing, and decision and display systems, electronic combat systems, and weapons guidance systems.

- Navy will develop a SEW-protect capability appropriate for joint and combined forces.

- As a matter of doctrine, future conflict, including SEW operations, will take place with combined arms.

- SEW will be coordinated both vertically (i.e., multi-echelon, from unified commander through tactical commander) and horizontally (i.e., across components in the force.)

- SEW will be conducted in terms of both warfare and warfare support functions within which are eight disciplines.

- Warfare support disciplines are:

  - Operational Security;
  - Surveillance;
  - Command and Control, Communications and Computers, and Intelligence (C^4I); and
  - Signals Management.

- The warfare disciplines of SEW are:

  - Operational Deception;
  - Counter-Surveillance;
  - Counter-C^4I; and
  - Electronic Combat.

- SEW undergirds all other mission areas. SEW enables targeting and prevents being targeted. To conduct SEW:

  - We will build a battle management system that is applicable across all echelons to all components of the force, regardless of position in it;

  - The system will incorporate a force-wide surveillance system, the interfaces of which are synergistic and seamless across the battle space and operationally transparent to the user regardless of echelon or component; and

  - The system will integrate hard kill, soft kill and very soft kill.

later emerged. With the airplane came volumetric battle space, and time became a significant factor in the naval equation. Anti-air warfare emerged, defined again by target set. (See Figure 1.)

Target	Doctrine
Ship	ASUW
Submarine	ASW
Aircraft/Missile	AAW
Decisionmaker	SEW

Figure 1. Warfare Areas By Target Set

At its simplest, the advent of SEW is both the recognition of the *requirement* and the achievement of the *means to* operate offensively and defensively in the electromagnetic spectra and in space and against the SEW target set. Like the other warfare areas, SEW contributes to Navy missions:

- To gain control of space and the electromagnetic spectra and deny or control the enemy's use of them;
- Having done so, to project power by conducting offensive warfare in those dimensions; and,
- Simultaneously, to protect our own SEW systems.

SEW IS JOINT

We must look beyond Navy resources alone to the force structure with which we will fight and with which hostile forces will fight.

Future conflict will take place with combined arms, and many future operations, as we saw in Desert Storm, will require an orderly transition from naval forces on scene to a combined force. Battle space for combined arms will include five environments—air, land, sea, space, and the electromagnetic spectra. This does not mean offensive warfare will occur in space. Rather, the interfaces of the five environments must appear seamless across both *echelons* and *components* in the joint (and combined) force.

When we consider the SEW target set in such a conflict, it is clear:

- SEW will be a joint endeavor;
- SEW will be conducted and coordinated both vertically (i.e., multi-echelon, from unified commander through tactical commander) and horizontally (i.e., across components in the force); and,
- The conduct of SEW typically will precede other actions on the tactical continuum.

Thus, like amphibious, strike, and anti-air warfare, SEW is a warfare area that in most future scenarios will extend beyond Navy and will require continuity of planning and action across echelons and components.

SEW DISCIPLINES

SEW includes both warfare and warfare support functions, contained within eight disciplines. (See Figure 2.) Warfare support disciplines are:

- Operational Security;
- Surveillance;
- Command and Control, Communications and Computers, and Intelligence (C^4I); and,
- Signals Management.

WARFARE SUPPORT	WARFARE
Operational Security	Operational Deception
Surveillance	Counter-Surveillance
C^4I	Counter-C^4I
Signals Management	Electronic Combat

Figure 2. SEW Disciplines

Operational Security consists of measures taken to minimize hostile knowledge of ongoing and planned military operations. It includes physical security, counterespionage, and personnel security.

Surveillance includes the tactical management of all technical surveillance as a *force system* across the entire multi-dimensional battle space, including all sensors, regardless of location (whether national, theater, or platform) or ownership (whether component, joint, or combined.)

C⁴I is the *means* to the *end* of command and control. C⁴I is a technological, organizational, and doctrinal system that provides three functions: the doctrinal delegation of forces (i.e., command and control); information management (i.e., communications and computers); and intelligence dissemination. Since World War II, the functions of command and control have been exercised through the system of C⁴I. Both command and control itself and the management of C⁴I systems, like aircraft, ships and weapons, can be delegated. It is important to recognize they are separate functions.

Signals Management encompasses measures to protect force signals and includes frequency management, signals security, communications security, computer security, transmission security, and emission control management.

The warfare disciplines of SEW are:

- Operational Deception;
- Counter-surveillance;
- Counter-C⁴I; and,
- Electronic Combat.

Operational Deception incorporates more than electronic deception. On the modern battlefield Operational Deception begins with diplomatic posturing, ends with technical reinforcement, and includes a multiplicity of actions in between. Operational Deception occurs in two phases, preparation and execution, and it is intended to influence enemy plans, execute a stratagem, induce reactions over a short period, and apply pressure to act. Operational Deception techniques are conditioning, reinforcement, and required continuity across echelons and components. Operational Deception is an essential element of every military action, and multi-echelon, multi-component coordinated Operational Deception is central to combined arms actions.

Counter-surveillance targets enemy surveillance systems. It is the sum of all active and passive measures to prevent enemy surveillance of selected areas. It consists of techniques to deny detection, divert detection, deceive or overwhelm the detector, and destroy it. Counter-surveillance is accomplished at all echelons, from unified commander and joint task force commander to component commander.

Counter-C⁴I targets enemy C⁴I systems. It includes measures to deceive, delay, degrade, or destroy elements of a hostile C⁴I system, including communications, data, and command and control nodes. It consists of techniques to deceive, saturate, jam, and destroy such elements. Like counter-surveillance, in modern warfare counter-C⁴I is accomplished at all echelons. (See Figure 3.)

Electronic Combat targets enemy weapons and weapon systems. It includes the coordination of all measures to provide counter-targeting/ counter-weapon, and terminal phase protection. An aim of Electronic Combat is to protect the force by providing a doctrinally organized, technologically seamless, area defense. However, unlike point electronic defense of today, Electronic Combat will accomplish that force defense through actions traditionally viewed as both *offensive* (e.g., destruction of enemy radars) and *defensive* (e.g., classical electronic counter-countermeasures) — the best defense is often offense.

NEW DIRECTION

Just as the airplane proved more than just better scouting for the battleship line in 1924, SEW is not just better electronic warfare or better C⁴I or better

Definition	Function	Means
Operational Deception • Is intended to influence enemy plans, execute a stratagem, induce reactions over a short period, and apply pressure to act	• To influence enemy plans, dispositions and expectations; • To induce reaction over a short period of time; • To apply pressure to act	• **Stratagem** (campaign level deception plan) • **Cover and security** (discourage interest) • **Feint** (maneuver before main operations) • **Technical deception** (stratagem continuity and reinforcement through communications; radar, navigation, recognition, acoustical, and electro-optical systems)
Counter-Surveillance • Targets enemy surveillance	• To deceive, degrade, evade, attack sensors and sensor platforms	• **Evasion and concealment** (denial of detection) • **Diversion and simulation** (divert detection) • **Deception** (technical means) • **Jamming and saturation** (overcome detector) • **Destruction**
Counter-C4I • Targets enemy C4I	• To deceive, delay, degrade, or destroy elements of hostile C4I from sensor platforms to weapons carriers • To deceive, delay, degrade, or destroy enemy command and control links and nodes	• **Deception** (manipulative deception of own communications) • **Deception** (imitative deception of hostile communications) • **Saturation** (overwhelm C2 systems) • **Jamming** • **Destruction**
Electronic Combat • Targets enemy weapons and weapons systems	• The coordination of all offensive and defensive measures across the force to provide counter-weapon protection to the force	• **Counter-targeting** (radar deception, IR deception, signals management) • **Counter-platform** (hard-kill request to ASUWC, AAWC, ASWC) • **Counter-weapon/terminal phase** (platform deception, decoys, jamming, hard-kill request to other commander) • **Jamming** • **Destruction**

Figure 3. SEW Warfare Continuum

utilization of space. Instead, like air power, SEW is a fundamental alteration of the tactical continuum that permanently has changed the face of naval warfare. Like the development of other new naval warfare areas in their time, it marks a collision between technology and doctrine, creating a new direction with revised tactics from what was previously evident.

The warfare opportunities offered by, and therefore, the drivers of SEW are:

- The potential to develop SEW weaponry;
- The systematic destruction or manipulation of hostile surveillance and command and control infrastructure prior to other tactical actions;
- The resulting separation of enemy forces from the decision-maker; and
- The potential to expand today's platform-specific electronic defense to a force-wide, counter-weapon defense covering a combined force across the entire five-dimensional battle space.

History does not teach that better technology necessarily leads to victory. Rather victory goes to the commander who *uses* technology better or who can *deny* the enemy his technology. The warfare support opportunities offered by SEW, therefore, are as significant as the warfare opportunities. They are:

- The doctrinal investiture in one commander of responsibilities in space and in the electromagnetic spectra that previously have been splintered among many;
- The conception of sensors—whether platform, theater, or national; component, joint, or combined—as a unified force surveillance structure; and,
- The development of virtual communications networks across multiple satellite communications coupled with a flexible command and control tailored broad applications.

Doctrinally, then, SEW not only adds to the tactical continuum through the first shots of Operational Deception, counter-surveillance, and counter-C^4I, but also adds an outer electronic layer of area protection through Electronic Combat. (See Figure 4.)

SEW TECHNOLOGY

Warfare in the modern world will be watched by the world, and "low-intensity" conflict is not the likely model. Instead, warfare will be characterized by intense, but calculated and discriminating violence—a small, but precise volume of fire aimed at creating a certain effect with timing and precision critical. The opening gambit and possibly the war termination strategy will be a SEW campaign focused on the decision-maker. Commanders likely will hold back no reserve, and surveillance will dominate their decisions.

What *technology* do we need to conduct this kind of warfare? At its simplest, there are three requirements.

First, we need a doctrinal, organizational, and technological battle management system that is applicable across all echelons to all components of the force, regardless of their position in it. The systems must be readily scalable across the levels of conflict as the force structure expands from battle group, Navy-Marine Expeditionary Force and joint task force to full campaign-level command like Desert Storm.

Second, the system must incorporate a force-wide surveillance system, the interfaces of which are synergistic and seamless across the battle space and operationally transparent to the user regardless of echelon or component.

Third, the system must integrate hard kill (e.g., weapons on target), soft kill (e.g., saturation,

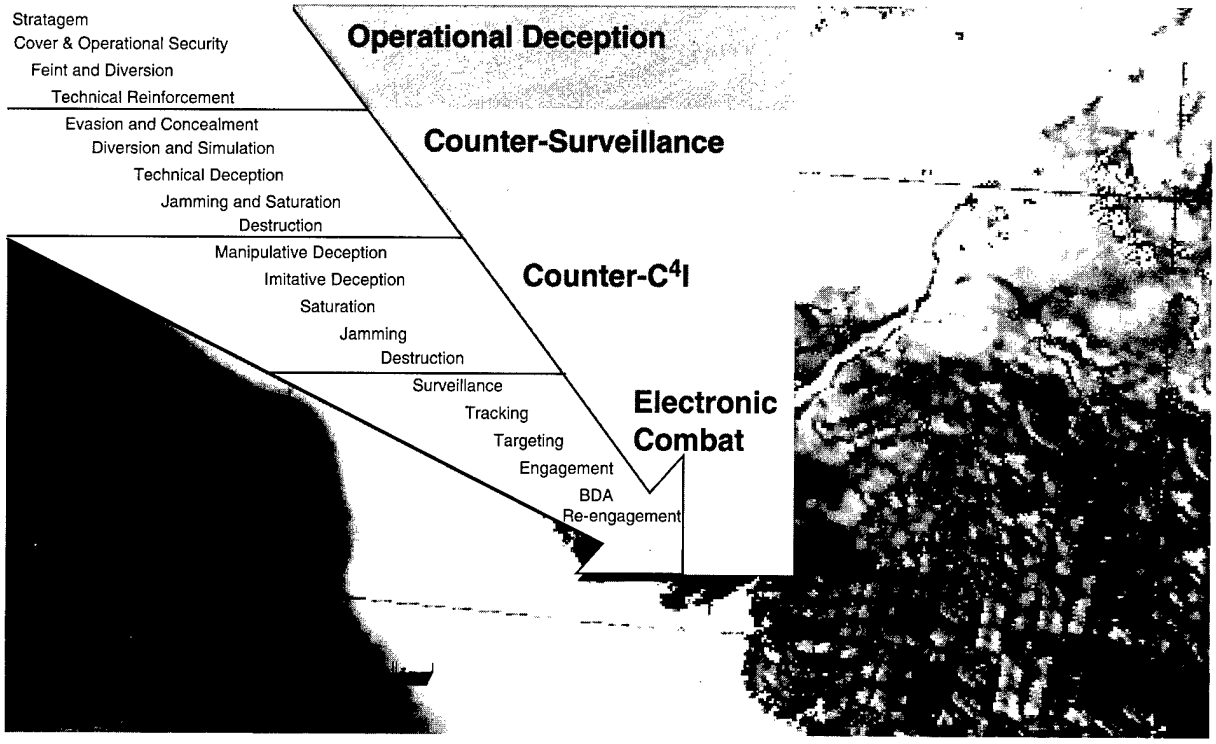


Figure 4. SEW Value-Added Provided by SEW to Tactical Continuum

deception), and very soft kill (e.g., intrusion). Such capabilities must be coordinated across the five-dimensional battle space and vertically up and down echelons.

Consider the major *technological* subsystems that must be built to conduct the eight *operational* disciplines of SEW in Figure 2. For warfare support, all four disciplines of which depend on technology to some degree. However, the magnitude of programs necessary to implement the Surveillance and C^{4}I system disciplines dwarf those of Operational Security and Signals Management. Similarly, constructing a viable Electronic Combat system will present the largest Navy challenge in the SEW warfare functions.

THE SURVEILLANCE SUBSYSTEM

Surveillance assets available to a commander of United States forces are programmed for and operated by diverse organizations. Some are part of a national inventory of sensors, others are operated at the theater level, others by allies, and still others are physically attached to tactical platforms.

The implication for joint warfare is that we require the means to sense the entire battle space as a whole, with transition across the air, land, sea, space and spectral interfaces transparent. Moreover, such a force surveillance system must be "borrowed" and focused on the tactical problem—that is, it is impractical and inappropriate programmatically for a component service to seek to construct such a force-wide sensor system. Instead, the question becomes: how can diverse sensors, many of which are neither owned nor operated by the commander, be focused sharply as a force surveillance system?

THE SURVEILLANCE GRID CONCEPT

The solution begins with a shift in perspective—away from the sensor itself to the battle space it senses. In making such a shift, we may conceive of the sensors as a grid of capabilities overlaying the battle space instead of a series of single sensors. (See Figure 5.) Such a grid would have variances over the battle space: number of sensors, detectables in the environment, location of sensors, their individual precision and resolution, and revisit times are some. By conceiving of sensors as a grid, we can arrive at some useful operational constructs.

First, at any given time or frequency, the variances could be seen as assets and lack of assets, which could be translated into probabilities when the grid is brought to bear against a track and then a targeting solution. Second, the precision of targeting solutions can be expressed relative to the weapon selected against the target instead of abstractly for any weapon. That is, the probability of target position only has to be as good as the guidance or the operator of the weapon needs it to be—an approach that will have an impact on weaponeering. Third, when we understand that sensors have operating envelopes as unique to them

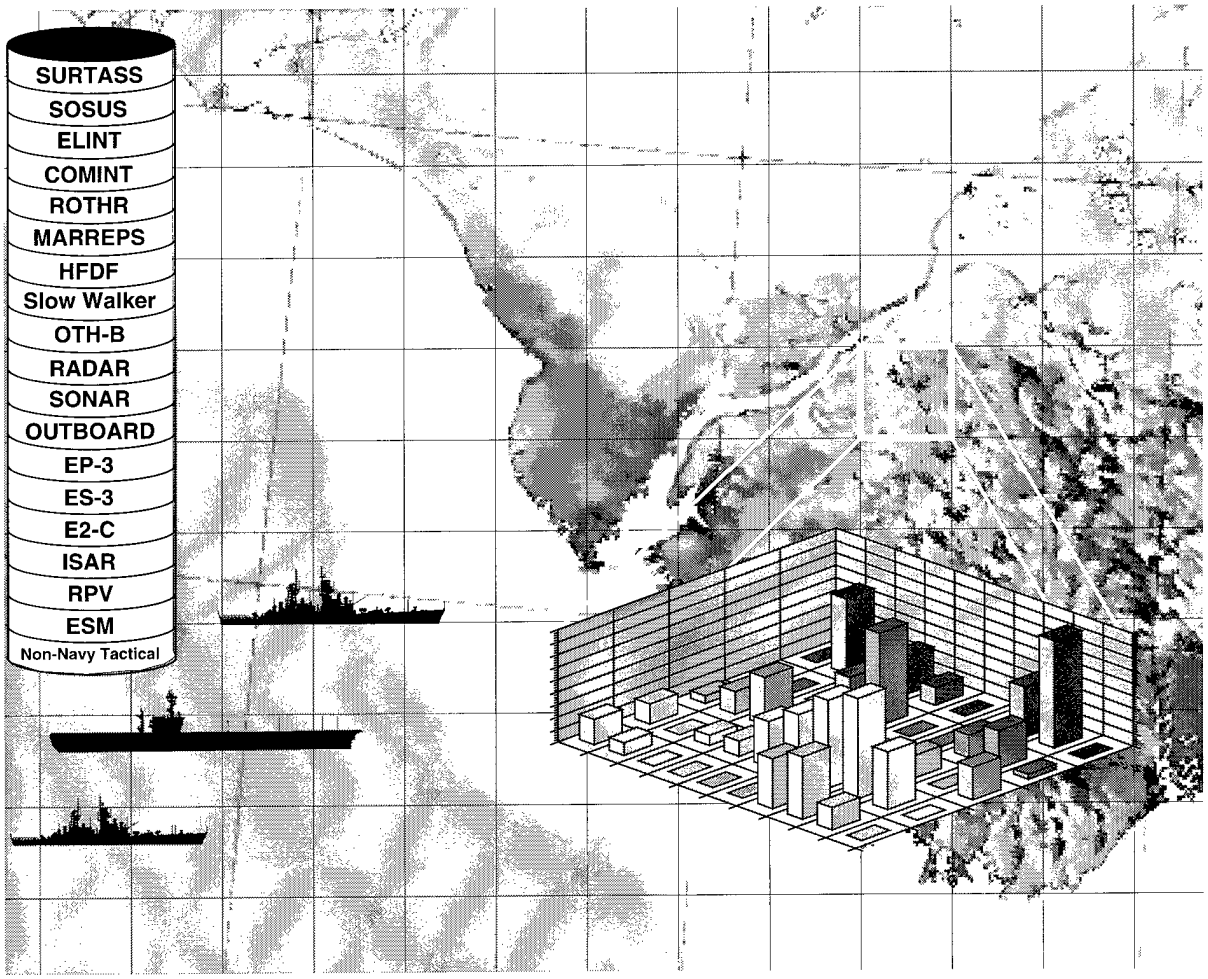


Figure 5. Multi-Spectral Sensing on Surveillance Grid

"THE CORE SYSTEMS"

The establishment of Space and Electronic Warfare as a formal warfare mission area stems both from the *recognition of the requirement* and the *achievement of the technological means to construct systems* which operate offensively and defensively in the electromagnetic spectra and in space. What are the Navy core systems needed to conduct SEW?

Future wars will be fought in coalition warfare with combined arms. The battle space will cross the boundaries of air, land and sea and extend into space and the electromagnetic spectra. Conflict, and the forces that fight the conflict, will be subject to escalation pressures ranging from diplomacy to logistics. SEW, therefore, is a joint and combined endeavor.

Much of the technology employed by opposing forces, certainly in space and the spectra, will be commercial and far more advanced than that available even in the last years of the 1980s. The impact will be both technological and operational: to pick a single example, a world in which U.S. forces are communicating on one transponder of a commercial satellite while a foe or the press uses another transponder on the same satellite requires a different view of counter-C4I than that held during the Cold War. Similarly, our approach to a SEW core system must be different than those envisioned for employment against the open-ocean, global threat of the former Soviet Navy.

In such a new world, as we have seen, three system requirements are overriding:

First, a battle management system that is applicable across all echelons to all components of the force, regardless of their position in it and capable of executing all eight disciplines of SEW;

Second, the system must incorporate a force-wide surveillance capability, the interfaces of which are synergistic and seamless across the battle space and operationally are transparent to the user regardless of echelon or component; and

Third, the system must integrate hard kill, soft kill and very soft kill.

Because of the complex battle space and the combined arms doctrine of the future, such a system must be capable of operating both independently as a Navy system, and seamlessly— as conflict and forces on scene escalate— as part of a larger joint construct (see below.) Programmatically, as well as operationally, Navy SEW core systems must be constructed as a fully compatible element of a larger joint construct. The reasons are manifest— force-wide surveillance capabilities, like communications satellites, do not belong to one military department; common technologies are necessary for information transfer; a force-wide Electronic Combat capability requires multi-component doctrine, standards, and goals; and so on.

While all eight disciplines require technology, it is possible to identify three major technological subsystems: Surveillance, C^4I, and Electronic Combat.

THE SURVEILLANCE SUBSYSTEM

Among the requirements for a Surveillance Subsystem are:

- A sensing capability across the electromagnetic and acoustic spectra, with a synergistic relation ship among platform, and Navy theater, and National sensors;
- It must be capable of identifying aircraft, ships, submarines, weapons, and hostile spectral emissions;
- The system must be flexible, scalable, and reconfigurable to be suitable for emerging threats and very high technology targets;
- It must be capable of supporting targeting over land and over sea; and
- Surveillance must be capable of being *perceived* by the commander as a single, albeit multi-component, system focused on the tactical operating area and be dynamically manageable regardless of the physical location of the sensor.

THE C^4I SUBSYSTEM

Among the C^4I Subsystem requirements are:

- A comprehensive, scalable command and control doctrine capable of supporting multi-unit forces from battle groups to Navy-Marine Expeditionary Forces;
- A multi-frequency, jam-resistant, satellite communications infrastructure including UHF, SHF, EHF military satellites and commercial satellites incorporating virtual networking and other capacity-saving measures;
- Communications must be capable of being *perceived* by the commander as a single, albeit multi-component, system focused on the tactical operating area and be dynamically manageable;
- New approaches to intraforce links that can support all Navy-Marine units across the air-land-sea interfaces and can support the common-force targeting requirements; and
- A system of analogous CINC command complexes ashore and Tactical Command Centers afloat that can be configured for diverse missions, share a consistent tactical picture, and impose information management techniques on the shore Global Information Exchange Systems.

THE ELECTRONIC COMBAT SUBSYSTEM

Among the Electronic Combat Subsystem requirements are:

- Comprehensive, scalable Electronic Combat doctrine and tactics, both offensive and defensive, capable of supporting multi-unit forces from carrier battle group to Navy-Marine Expeditionary Forces; and
- The development of an SEW battle space modeling capability that is dynamically updated by reconfigurable ESM and other sensors from the Surveillance Subsystem and capable of executing ECM/ECCM measures across the force.

as those of a particular aircraft, such a grid can be manipulated effectively, and perhaps dynamically, to compensate for complete "holes" or unacceptably low probabilities.

Conceptually, the enemy also has such a surveillance grid. Similarly, his grid can be studied, with strengths and weaknesses becoming apparent to the U.S. SEW Commander. By such a conception, we can consider and exploit in detail the symmetries of SEW and reduce its complexity to doctrine (in this case surveillance and counter-surveillance.)

How could such a grid be "constructed"? There are six keys:

- The organizational focal point from which to operate the grid. This is the SEW Commander concept;
- Personnel with experience and training to understand the sensors and the grid;
- Display tools to visualize the sensor output conceptually as a grid over the battle space and to monitor perturbations in the grid and from which to task the grid;
- Algorithmic and other technical tools to relate disparate sensors;
- The sensors; and
- Software bridges to translate the various sensor output into a common, digital format.

THE COMMUNICATIONS GRID

In the same way we can conceive of a surveillance grid, we can also conceive of a communications grid. Unlike surveillance, however, this has only become possible recently and will not be a mature capability until the end of this decade. In the last 20 years, military communications, especially satellite communications, kept pace with and were often ahead of commercial communications. In the past decade, however, the worldwide telecommunications revolution has exploded, and it is clear today that a robust communications infrastructure will be available globally by the turn of the century. Moreover, military satellite communications have expanded as well. The Navy UHF Follow On constellation, the installation of SHF DSCS antennas on major combatants, and medium-data-rate Milstar are more than quadrupling capacity. A military communications technician who retired in 1988 and one on active duty in 1995 will have worked on entirely different communications infrastructures.

Not only are the number of communications transponders increasing, but breakthroughs in multiplexing, the move to digital formats, and, most importantly, the advent of virtual networking will provide military commanders with a communications capability that not only will be jam-resistant (by virtue of network switching) but also several orders of magnitude larger.

By the close of the decade, both the U.S. commander and a hostile commander can expect robust communications with restoration options and, with the advent of computer workstations, flexible command and control. But clearly, these capabilities—because of the footprints of satellites and the geography of the battle space, including the shore infrastructure (e.g., the local telephone services)—will vary from place to place on the globe. Thus, as with sensors, we may appropriately conceive of communications as a grid overlaying the tactical area—again, both a friendly grid and a hostile grid.

How could such a grid be "constructed"? Three things are needed:

- The organizational focal point from which a grid is operated. This, again, is at the heart of the SEW Commander concept;
- Display tools to visualize the communica-

tions networks conceptually as a grid over the battle space and to route, restore, and task the grid; and,

- A system of communications pathways that are common and transparent to the operator.

THE C⁴I SUBSYSTEM

Having conceived of operating sensors and communications as grids over the tactical area, how can the move be made from conception to a tangible operating system? To do so, we need to remember that both grids are comprised of assets that actually are geographically diversified. The surveillance grid contains national, theater, and platform sensors from all four services and the allies. The communications grid contains virtual networks within the tactical area as well as global networks.

In conceptual terms, we ask ourselves how we can move sensor information from the surveillance grid to the communications grid to further route it to the tactical user. If we consider the surveillance grid as a system, the inputs to the grid are emissions sensed, and the outputs today are typically messages of one format or another. With the exception of platform sensors, the message output moves into the military communications system for transfer to the tactical commander. The number of national sensors and theater systems are small and finite, just as the number of detectable emissions in the tactical areas are (relatively) small and finite. Moreover, the emissions often have a mathematical relationship to the emitter, which in today's C⁴I system is not usually apparent because the user sees the emissions as multiple, often redundant, messages that are difficult to correlate.

A reasonable technological analogy to employ for our current sensors is that of an automatic rifle firing bullets into a brick wall. In terms of technology, the sensor reports (i.e., the bullets) are being produced by computers that operate typically in millions of instructions per second (in some cases, billions) but are being disseminated in communications systems with processors in the range of thousands of instructions per second. There are two other serious problems.

The second is the communications output bears no relationship to operational reality—that is, the number of messages sent per emission sensed not only is not one for one, but often literally is unknown. It is this problem that makes fusion so difficult. An initial sensor report that enters the communications system produces multiple messages like a cue ball scatters a rack of billiard balls.

The third difficulty (which we will turn our attention to in detail later in this paper) is that platform sensors, except those with access to the service specific links, could not today be part of the surveillance grid *because their output is not shared with other platforms.*

If we can solve these problems, we provide the tactical user with the capability to operate these complex and diverse parts as whole grids. For these reasons, Navy C⁴I was restructured around the Copernicus Architecture.

Under the Copernican concepts, the sensor outputs will be routed into a series of Global Information Exchange Systems (GLOBIXS), networks that will be terminated into a CINC Command Complex (CCC). At the CCC, each GLOBIXS will be "anchored" by a staff experienced in the GLOBIXS discipline (e.g., SIGINT, ASW). (See Figure 6.) Through this "anchor," the tactical commander may delegate responsibility for selected sensor output rather than manage it all himself. This would be achieved doctrinally through the CCC anchors and technologically by setting filters that limited data parametrically, geographically, temporally, or administratively.

This provides the tactical commander, for the first time, the capability to delegate responsibilities ashore in the same way he has always delegated responsibilities afloat and takes full recognition and

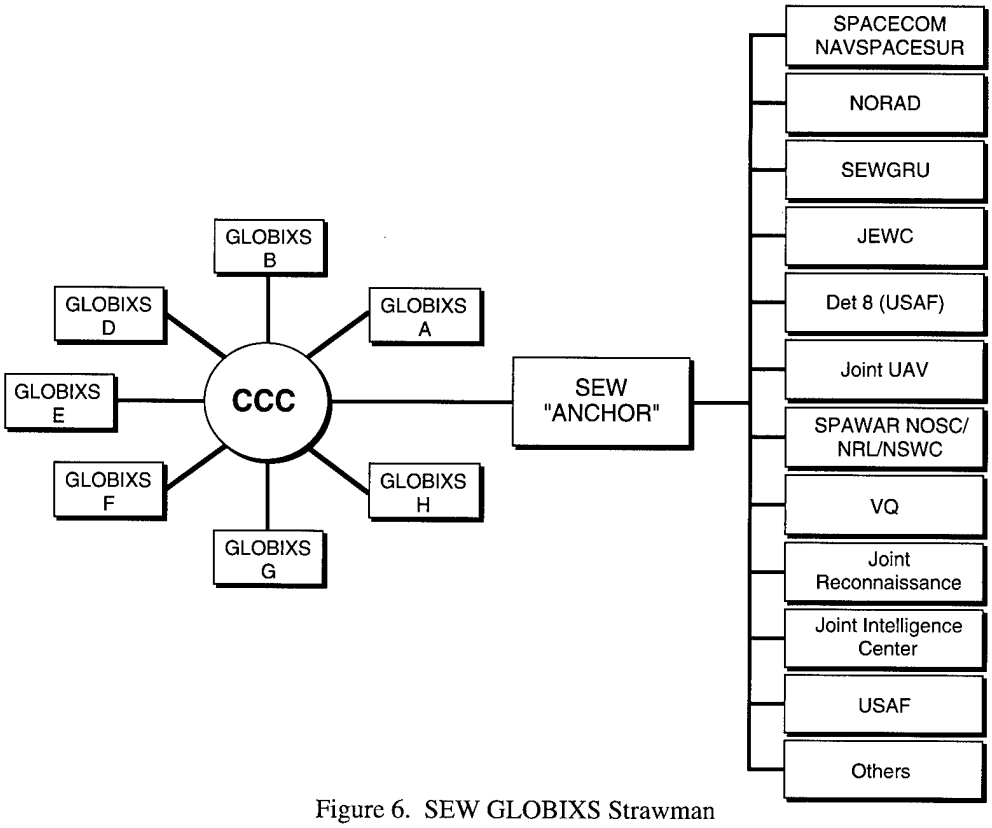


Figure 6. SEW GLOBIXS Strawman

account of the critical role the shore establishment plays in modern warfare.[1]

From a technological perspective, Copernicus was designed to solve the other key problems necessary to operate sensors and communications as tactical commander's grids. Sensor traffic that enters the GLOBIXS will be format-converted into a common digital sensor report called Copernicus Common. (See Figure 7.) This common sensor report structure would be used for any sensor, whether national, theater, or platform and would be addressed to platforms that have been assigned to receive it (via the force commanders' C^{4}I plan.) Sensor data arising from force sensors or from GLOBIXS (i.e., shore-based sensors) would be distributed to the force one time in one format via Tactical Data Exchange Systems (TADIXS.)

An emission, regardless of whether it was collected by a platform or national sensor, will be reported to the tactical force in a common format, on a bit-oriented, true-navigation display over communications pathways selectable by the commander. Thus, the location of the sensor and the location of the communications transponder are transparent to the operator.

It is the C^{4}I system, then, designed to make communications transparent to the user and all sensors available in common formats, that allows us to conceive of the Surveillance and Communications Grids and of information movement between them.

[1] Through this delegation, the Copernican precept of "pulling" information to the user instead of "pushing" information at him was derived. It is important to note, however, that there are significant operational considerations in doing so. For administrative traffic, setting the wrong "pull" parameters could potentially have annoying or even costly implications to the user who set them. But for sensor traffic, the ramifications are serious, and the need for an experienced anchor on these GLOBIXS. The ASW, SEW, or SIGINT anchor ashore, regardless of geographical location, is a key player in the tactical battle space.

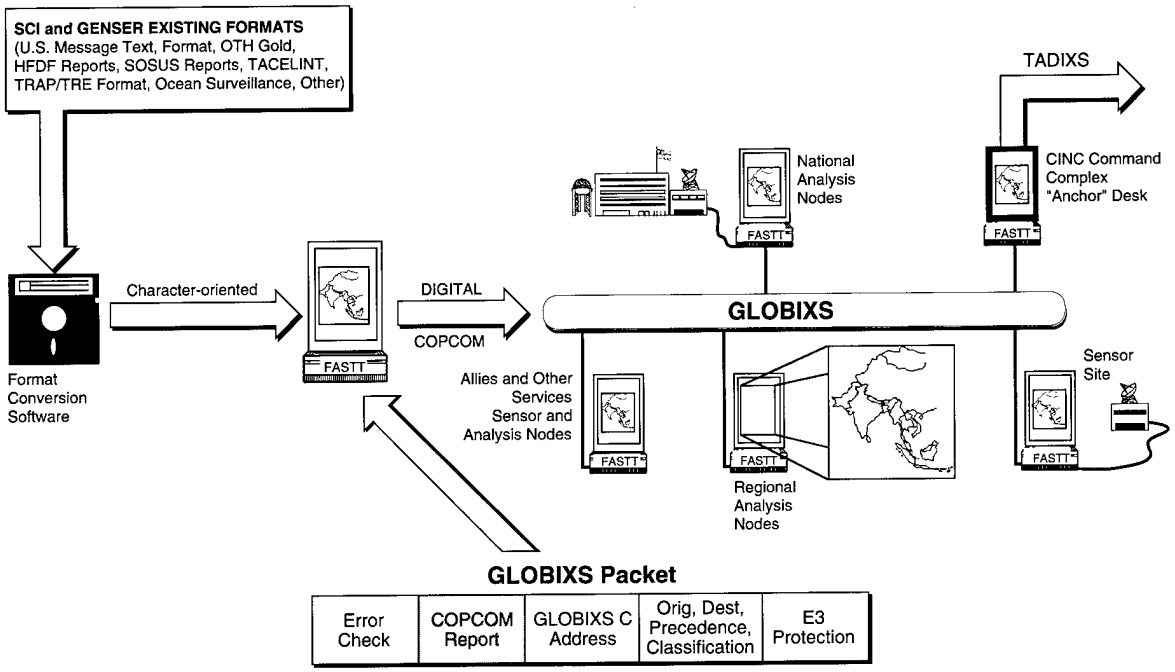


Figure 7. Converting Sensor Reports to a Common Digital Report on GLOBIXS

SEW BATTLE SPACE MODELING

A ravenous requirement for information exists. The implication of fighting with one coalition against one hostile force in one theater in one year and with another coalition against a second hostile force in another theater in another year is that data of every kind (intelligence, environmental, political, diplomatic, parametric, geographic) will be at a premium. This problem will be compounded by the proliferation of all makes of weaponry in the world and the commercial explosion of telecommunications and computing equipment. Future hostile arsenals will not be as homogenous as those of the former Soviet Warsaw Pact.

Nowhere will data be more critical than in Electronic Combat, the third major technological subsystem of SEW, which is fought in battle space difficult to perceive and even more difficult to understand.

Consider a clear blue October afternoon: it is as though there was no atmosphere. It appears nonexistent. If we return to the same building in January, the winter sky allows us to see the currents and eddies of the atmosphere and understand its topography. The same is true for the electromagnetic spectra—we need a way to operate in it understanding it as a January sky while showing the enemy hostile commander only the October transparency.

In that sense, operating in the SEW battle space is much like the submarine battle space. Similarly, Electronic Combat—a composite of doctrine, organization, and both offensive and defensive tactics—is analogous to submarine water space management. And, like the subsurface environment, humans lack the sensorial means to "see" the SEW battle space — to operate in it, we must develop the means to perceive it and deny its perception to the enemy.

The complex SEW environment, which is created by machines, must be modeled to be understood by humans. And the resulting model, because of the factors that influence the electromagnetic spectra, must be a complex composite of six tiers (see Figure 8):

- The first tier is the geographic model. To conduct SEW in New Guinea is to operate in a different electromagnetic environment than in the New Hebrides;
- We must add to the geographic mode the physical environment, which perturbates the spectra;
- Onto that must be added the sensed model, which contains information about hostile platforms, sensors and weapons and the electronic equipment they use; and
- The fourth tier is the own force model, which provides similar data for friendly forces to that of the sensed model.

At this juncture, the model being developed is a useful one for any warfare area, not just SEW. If we add to these four tiers of modeling two more — an expert model through which we impose our doctrine, and a technical parameters model through which we compare and assign targets to weapons— we can arrive at a specific warfare mission model. Using our existing doctrine as a model, we could proscribe models for SEW, strike, anti-air warfare, anti-submarine warfare, amphibious warfare, and so on. (From a joint perspective, such modeling presents powerful opportunities for joint task force (JTF) management and could provide the technological basis for more capable JTF command and control.)

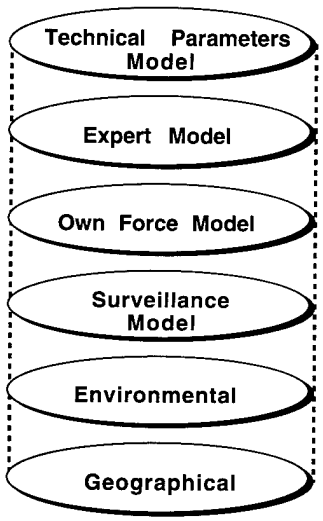


Figure 8. Building the SEW Battle Space Model

What does it take to build such modeling capabilities? Two things: a computing capability to generate and maintain the model and the information infrastructure to feed the model dynamically. The first is glaringly missing from our naval or military platforms today—it is a functional design hole. While computer-assisted systems abound, they are focused on discrete tasks. Even workstations, which have brought about major improvements in command and control, are employed in the limited tasks such as display and correlation. What we are missing is a cerebral computing function, which although distributed in design, we may call "main computer." We may envision main computer functions at the shore Copernicus CCC and main computer functions at the TCC as analogous and consistent with the Copernican goals of common, consistent tactical pictures ashore and afloat. Although a main computer would have many functions, relative to SEW it would:

- Generate the models discussed above;
- Provide a computing capability to conduct SEW through the four techniques discussed below; and,
- Provide the interface between external communications (TADIXS) and internal communications (Combat Direction System [CDS].)

SEW TECHNIQUES

SEW, as we have seen, has warfare functions and warfare support functions. So too, does SEW modeling. If we can develop a model of the SEW battle space, then conceptually we can model the hostile perception of that same battle space and begin to make offensive decisions about where, when, and how to disrupt it or how to change his perceptions. Thus, the ability to model the SEW battle space dynamically not only is critical to SEW warfare support functions, but also to the SEW warfare functions of Operational Deception, counter-surveillance, counter-C^{4}I, and Electronic Combat. Beginning with a setpoint model (i.e., the SEW model at a certain time), we can describe four sequential and repetitive techniques by which we conduct SEW.

Model formulation, then, is the first SEW technique. The second technique is to replicate the hostile SEW systems. At first glance this seems simple; however, in the modern world it is a very complex task—when we consider the sheer scope and magnitude of SEW systems (e.g., sensors, communications, command and control nodes, links, weapons guidance, hostile counter-electronics equipment.) The purpose of replication is to gain a high order look at hostile systems—what sensors, what C^{4}I capabilities, what nodes and links are present. Through replication, the levels of SEW (i.e., what echelons are assigned which SEW tasking) can be planned before hostilities begin—*for SEW is as much operational art as tactics.* Decisions as to what hostile SEW systems to attack are addressed at this stage in planning (e.g., whether to attack surveillance or communications or both, and what residual capability to leave the enemy in order to conclude the conflict.)

The third step is to devolve the replicated hostile systems through a technique contained within the main computer called "hypersearch." Hypersearch uses object-oriented analytic capabilities to descend and transverse the information layers of a complex technical problem. (See Figures 9 and 10.) In deciding to attack the hostile C^{4}I system, hypersearch is the logical process of attempting to retrieve detailed information on that overall system: what communications subsystems, what commercial satellites, what satellite terminals, what terminal manufacturer, what software, how

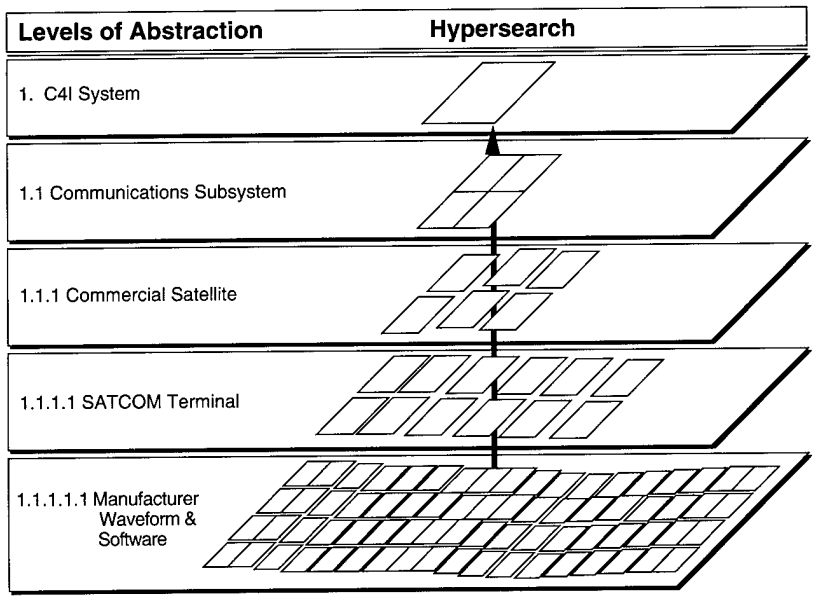


Figure 9. Hypersearch

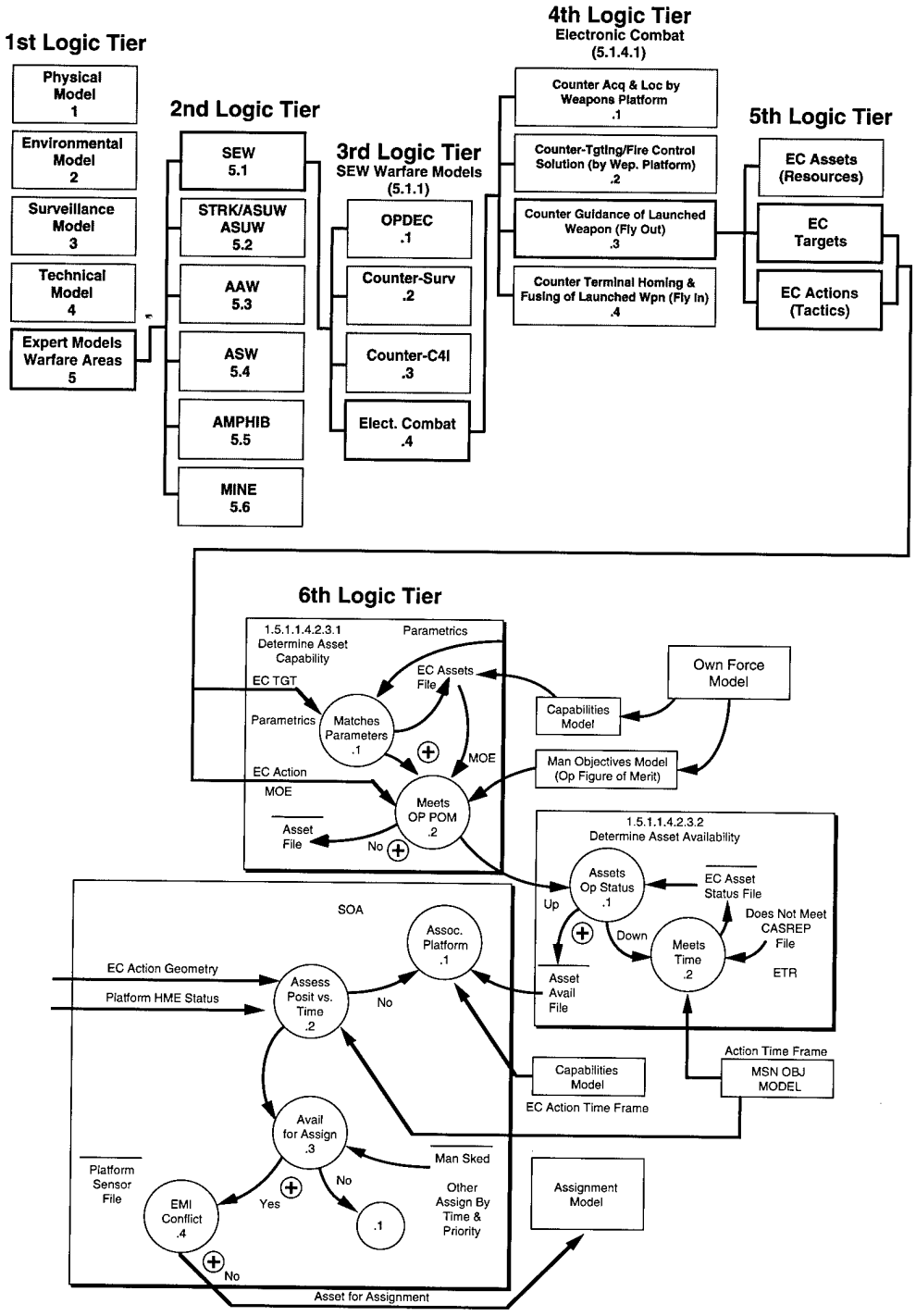


Figure 10. Hypersearch and Modeling Combined for Electronic Combat

many lines of code? Hypersearch seeks to find the appropriate target set to destroy the C^4I system. For example, while the C^4I target set theoretically could range from targeting satellites to antenna fields to software viruses—the simplest, most effective solution might be to target a bridge under which runs the principal fiber optic cables between command and control nodes. Or, the same decision could be made in order to drive the enemy to radio, where SIGINT collection, possibly leading to a counter-surveillance operation, might take place.

The final step, which follows from determining the target, is to select and apply the kill. In SEW warfare, applying the kill means selecting a weapon set (i.e., to request a hard kill, or apply a soft or very soft kill), as well as the echelon, component, and platform that has the weapon.

THE ELECTRONIC COMBAT SUBSYSTEM

The purpose of the Electronic Combat system is to devise a means to put in place an electronics capability across the force, rather than only around specific platforms within the force. The goal of Electronic Combat is to provide counter-targeting and counter-weapon protection for the force, recognizing the force likely will be joint and combined and operating throughout the five-dimensional battle space. Such a concept is revolutionary and seems at first glance to require major technological innovations. However, we do not mean to construct a technological panacea or develop a new type of electronic shield. We mean instead to devise a coordinated doctrinal, organizational, and technological system that can interleave and operate diverse capabilities from platform counter-electronics suites (e.g., SLQ-32, chaff) to electronics counter-measures missions (e.g., SEAD) as a synergistic whole, across a combined force, across a multi-dimensional battle space. Such an Electronic Combat subsystem would have several main attributes:

- Doctrine developed to operate such a system;
- An organizational focal point to task and manage Electronic Combat;
- Like sensors in the surveillance grid, the Electronic Combat subsystem must be *programmable*—for, the implication of heterogeneous hostile forces is that these electronic order of battle is potentially more diversified than that of the former Warsaw Pact nations; and,
- Similarly, a set of tactical standards for platform Electronic Combat systems must emerge so that individual components can fit seamlessly into a whole force system. This is analogous to communications and protocol standards in information systems.

We are some distance from building such a system, yet not as distant as it may initially appear. If we recall the analogy of the office building window in January, we are contemplating the kind of perception we must have of the spectra to construct an Electronic Combat subsystem. In reality, it is little different than building an AAW system; it is simply that as humans we can perceive of the target in AAW more concretely than we can in Electronic Combat. To make that winter sky perceptible, there are two additional requirements for Electronic Combat, one which we have discussed, and another which we will set down in the paragraphs below.

- The fifth requirement is the ability to model the SEW battle space dynamically so that we have a continually changing tactical picture of the Electronic Combat threat and order of battle. Such a model provides Electronic Combat targeting and post-Electronic Combat BDA. This capability we have described in the main computer function; and,
- Finally, it must operate a force-wide system, and we must find the means to link diverse platforms together.

THE TACTICAL GRID

There are three fundamental changes in U.S. tactical force structure in the post-Cold War. First is, the expansion and contraction of combined arms forces from on-scene presence (e.g., carrier battle group) to JTF to full unified command as the crisis transitions to war. Build up and build down require smooth transitions, and pose not only challenges in logistics but also in warfighting doctrine. Second, there will be a merger of air, land, and sea warfare into the common battle space of a post-Cold War campaign. Finally, there is a need to operate with one coalition today and another tomorrow.

These three changes in force structure point to a common question: how do we construct joint and combined forces with a plethora of platforms in a seamless multi-dimensional battle space—and do so with one force in one place one day and a different force in a different place on the next?

The answer lies in another shift in perspective, this time to new concepts in tactical links. Today, if we used the concepts of a Surveillance and Communications Grid, they would be useful but limited constructs because they terminate over *one platform at a time*. Our ability to construct and command a force depends ultimately on our ability to link them together tactically. Current link technology is not universally shared among the services and the allies, and that we which we do share is technologically inadequate (e.g., Link 11) and usually application-specific (e.g., JTIDS). Making the various tactical elements in Desert Storm operate and function as a force was accomplished, but only imperfectly because information could not be shared across the force.

As a force-wide requirements model for tactical information, none is better than the Aegis model of "data base" separated by the thinnest interface with the fire control solution. (See Figure 11.) By data base the Aegis model means that information necessary to derive the fire control solution. If we translate that model to the terms used in this paper, the Surveillance Grid and the Communications Grid bring us to that interface above the fire control solution. At that interface, we are forced to ask ourselves two questions.

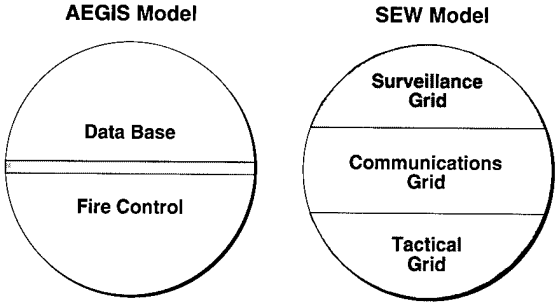


Figure 11. Aegis and SEW Battle Management Models

The first is, how can platform-external information from the Surveillance and Communications Grid be parsed with own-platform information—which is to say, what is the nature of the Aegis model interface? Without an adequate answer to this question, two serious problems arise:

- The Surveillance and Communications Grids become solely non-organic grids; and,
- Fire control solutions (i.e., weapons) are irreconcilably separated from "data base" information.

To a great degree, this situation is, in fact, what we experience today in our current platforms.

The second question is, how can platform information be shared from platform to platform? *Without an adequate answer to this question and the first, we cannot operate joint/combined force in a seamless battle space*. This is also, in fact, what we experience today. Different components take non-organic information into the force in different ways than other components, and the exchange of organic information among components is virtually nonexistent.

It is these two central questions that —asked in the context of joint and combined warfare in multidimensional battle space and coupled with the need to construct a force wide Electronic Combat system—lead us to the three overall requirements previously stated and repeated here for a battle management system:

First, we need a doctrinal, organizational, and technological battle management system that is applicable across all echelons to all components of the force, regardless of this position in it. The systems must be readily scalable across the levels of conflict as the force structure expands from carrier battle group, Navy-Marine Expeditionary Force and joint task force to full campaign-level command like Desert Shield/Storm.

Second, the system must incorporate a force-wide surveillance system, the interfaces of which are synergistic and seamless across the battle space and operationally transparent to the user regardless of echelon or component.

Third, the system must integrate hard kill (e.g., weapons on target), soft kill (e.g., saturation, deception), and very soft kill (e.g., intrusion). Such capabilities must be coordinated across the five-dimensional battle space and vertically up and down echelons.

These considerations bring us to the final SEW construct: the Tactical Grid. The Tactical Grid is conceived as a wide-area Combat Direction System (CDS), a network of small communications links that tie all units of the force together regardless of platform or component. If we return to the Aegis model, the differences between the Communications Grid and the Tactical Grid become evident. The Communications Grid provides Copernican TADIXS connectivity (the Aegis data base category), which facilitates information moved among operators and analysts. The Tactical Grid, alternatively, connects CDS systems among units of the force in order to provide fire-control-grade information across the battle space.

A good analogy for the Tactical Grid is a power grid. When computers of different makes and operating systems are plugged into electric power outlets, they get a common "fire control" solution. With the Tactical Grid, we can go much farther. By connecting CDS systems across the force—across the air, land, sea interface—we also are connecting platform sensors, weapons batteries, main computers, and electronic combat suites into the force-wide system. Because of this capability, we can construct the force-wide Electronic Combat subsystem described above, which can be tasked and managed.

Thus, the Aegis model is compatible with the SEW model, but the SEW model properly is anchored on the battle space instead of an engineering goal. The Surveillance Grid ties together all available sensors, exchanges information from them over the Communications Grid (using the Copernican GLOBIXS and TADIXS), and crosses over to weapons systems through the main computer functions onto the Tactical Grid as a fire control solution. Thus, we should think of two kinds of communications networks in the future: TADIXS, which provide battle management information, and the Tactical Grid, which provides platform sensor and fire control information. (See Figure 12.) The Tactical Grid is envisioned as a small, but very jam-resistant link, over which three specific kinds of information would be exchanged:

- Own unit's sensor data, which would be fed into the grid as raw material for force track managers to capture potential all-force use;

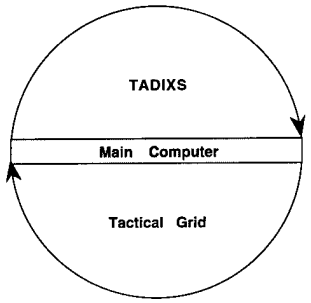


Figure 12. TADIXS and the Tactical Grid

- "Real" track plot (or rather "approved" tracks) from the force track managers that provided the Grid solution; and,

- Perhaps a small vocabulary of instructions by which sensors and Electronic Combat suites can be tasked or focused force-wide.

Because of the presence of main computer, the Tactical Grid would move information in "Delta" packets, or a compressed digital format that would send only sufficient information to unlock a data record in the recipient computer. (That is, rather than send all information on a target, a Delta packet might send only a previous track number, a new position, and an assignment.) Because of the need to include an ally in one mission and exclude the same ally in the next mission, the Grid cryptography would be over-the-air rekeyed and probably employ a transmission security (frequency-hopping) module.

Operationally, the impact is that a B52, a Danish frigate, and a Abrams tank can be connected to the Tactical Grid imposed over the operating area like joining a regional power grid. This link would occur simultaneously with TADIXS linkups, allowing the operators of those platforms to plug into the Surveillance and Communications Grids (i.e., the Aegis data base) as well as the Tactical Grid (i.e., the Aegis fire control.)

THE SEW COMMANDER

Whether he conceives of it that way or not, when a tactical commander begins his operation and turns his attention to communications, to surveillance, to electronic warfare, to Operational Deception—he is conducting Space and Electronic Warfare. The issue is not whether SEW is needed; it is here. The issue is how best to conduct it, exploit it, and manage it.

Moreover, whether he conceives of it or not that way, the tactical commanders problem relative to SEW is to manage the three "grids" described in this white paper. Thinking of the diversity of sensors, communications, and weapons systems as grids overlaid on the tactical battle space is simply a more readily understandable and more useful way of viewing the myriad of assets involved in SEW.

But a grid conception is only part of making the complexities of SEW systems easier to operate: it is not technology alone that makes SEW a system or that makes SEW seamless. SEW as a warfare area, like all warfare areas, depends on four factors: the establishment and implementation of workable doctrine; the articulation of and subsequent building of achievable technological subsystems that can operate together as a whole system; the education and training of officers and sailors who understand SEW operationally and technologically; and finally, a supporting infrastructure of organizations, including those involved in programming, engineering, and operations, that can plan, build, and conduct SEW.

In the historical establishment of all previous warfare areas, these four criteria have been necessary—and were met—before success was achieved. Yet, none were achieved by walking to a blackboard and methodically planning each of the four requirements. It is a true statement, but not an indictment, that the Fleets of the world never had a formal requirement for an airplane, or a submarine, or a communications satellite. Instead, in all cases, a debate was established within the Fleet (indeed, within the Fleets of the world) and over time doctrine, technology, people and organization came to fruition. So will it be with SEW.

Nonetheless, the debate must begin on a sophisticated footing, and SEW, like all warfare areas, begins with an understanding of what the warrior *must do*. By understanding what the warrior does, we can see what kind of warrior we will have to mold. Therefore, it is fitting in this paper, which has focused heretofore on doctrine and technology, to close on a discussion of the human functions of SEW and, therefore, what the SEW Commander's responsibilities must be.

When a SEW Commander exercises his

responsibilities, he will do so in the dichotomy of warfare functions and warfare support functions. The grid construct serves us well here. For if we can conceive of own force SEW assets as three grids over the operating area, then the SEW Commander's support functions reduce themselves to managing a "core sample" through all three grids in a manner that provides operational continuity vertically through them. If we have weapons and communications, but no surveillance, we cannot fire the shot. This situation occurs today (though we may not recognize it as a grid problem) when the revisit time of a sensor will not allow us to target. If we have surveillance and weapons, but we cannot connect the two, the solution is still zero. This is what we experience in today's non-virtual, circuit-specific communications when a targeting network fails. Similarly, surveillance and communications are no good without the weapons. This is the situation when a CDS failure occurs or when a targeting solution cannot be passed to the optimum shooter.

Thus, one part of the SEW Commander's role is to manage the own's force grid continuity. But if we can conceive of grid for us, we can also conceive of analogous hostile grids and devise to disrupt their continuity. The techniques of doing so we have discussed previously: modeling, replication, hypersearch, and kill application.

FOUR FUNCTIONS

We may, therefore, describe the SEW Commander's functions as four. (See Figure 13.) First, force sensor management—which is to say, Surveillance Grid integrity. The functional responsibilities include sensor management, collection management, and surveillance coordination for the echelon in which the SEW Commander is positioned (i.e., Navy CVBG, JTF, theater). The person assigned these functions must have an operational and technological understanding of all sensors that can impact the battle space—national, theater, platform; allied, component or joint; friendly or hostile.

Second, the conduct of Electronic Combat. The functional responsibilities include maintenance of the force-wide electronic combat capability

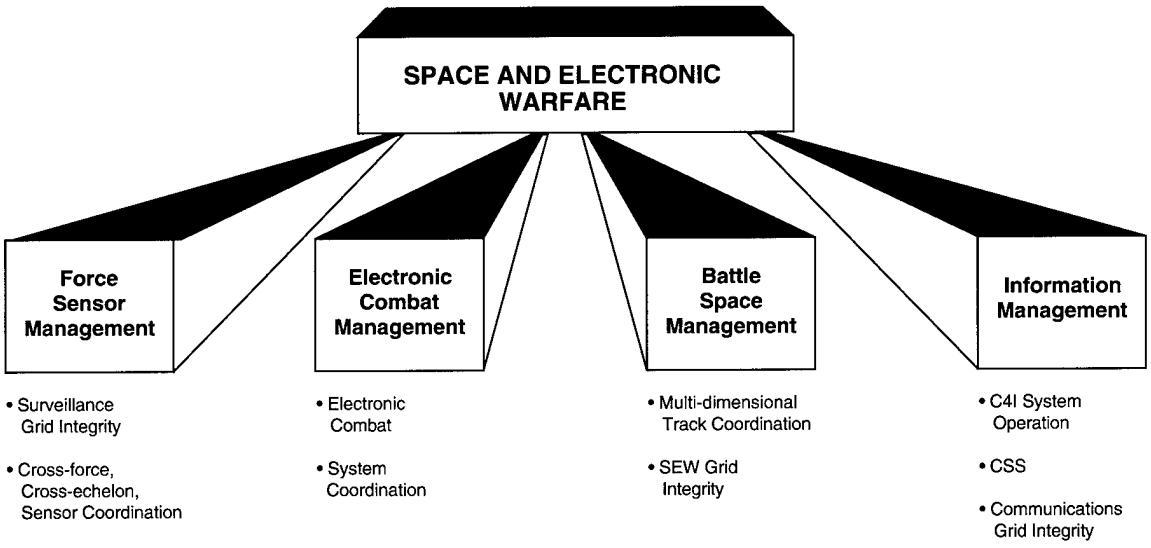


Figure 13. SEW Commander Functions

previously described. The person assigned these functions must have an operational and technological understanding of all electronic systems that can impact the battle space—national, theater, platform; allied, component or joint; friendly or hostile.

Third, battle space management. The functional responsibilities include track and targeting coordination throughout the battle space, whether air, land, sea, or space—which is to say, Tactical Grid integrity. The person assigned these functions must understand weaponry and surveillance—national, theater, platform; allied, component or joint.

Fourth, information management. The functional responsibilities include managing the Communications Grid, the virtual networking that rides over it, and the Copernicus C^4I system. The person assigned these functions must understand communications—national, theater, platform; allied, component or joint; commercial and military; and friendly and hostile jamming and interference potentials.

GLOSSARY

AAW	Anti-Air Warfare
AAWC	Anti-Air Warfare Commander
ASMD	Anti-Ship Missile Defense
ASUW	Anti-Surface Warfare
ASUWC	Anti-Surface Warfare Commander
ASWC	Anti-Submarine Warfare Commander
ASW	Anti-Submarine Warfare
BDA	Battle Damage Assessment
C&D	AEGIS Command and Decision
C2	Command and Control
C^4I	Command and Control, Communications and Computers, and Intelligence
CCC	CINC Command Complex
CDS	Combat Direction System
CINC	Commander-in-Chief
COMINT	Communications Intelligence
COMPUSEC	Computer Security
COMSEC	Communications Security
COPCOM	Copernicus Common
CSS	Communications Support Service
CVBG	Carrier Battle Group
DSCS	Defense Satellite Communications System
EC	Electronic Combat
ECCM	Electronic Counter Countermeasures
ECM	Electronic Countermeasures
EHF	Extremely High Frequency
ELINT	Electronic Intelligence
EMCON	Emission Control
ESM	Electronic Warfare Support Measures
EW	Electronic Warfare
FASTT	Fleet All-Source Tactical Terminal
FOTC	Force Over-The-Horizon Coordinator
GENSER	General Service
GLOBIXS	Global Information Exchange Systems
HFDF	High Frequency Direction Finding
JEWC	Joint Electronic Warfare Center
JIC	Joint Intelligence Center
JTF	Joint Task Force
JTIDS	Joint Tactical Information Distribution System
LPI	Low Probability of Intercept
MEB	Marine Expeditionary Brigade
MEU	Marine Expeditionary Unit
MIJI	Meaconing Intrusion Jamming and Interference
NAVSPACESUR	Navy Space Surveillance Center
NORAD	North American Aerospace Defense
OPSEC	Operational Security

OPDEC	Operational Deception
OTH-GOLD	Over-the-Horizon GOLD
ROTHR	Relocatable Over-The-Horizon Radar
RPV	Remotely Piloted Vehicle
SCI	Special Compartmented Intelligence
SEW	Space and Electronic Warfare
SEWC	Space and Electronic Warfare Commander
SEWGRU	Space and Electronic Warfare Group
SHF	Super High Frequency
SIGINT	Signals Intelligence
SIGSEC	Signal Security
SOF	Special Operations Forces
SOSUS	Sound Surveillance System
SURTASS	Surveillance Towed Array Sensor System
TACELINT	Tactical Electronic Intelligence Report
TADIXS	Tactical Data Exchange Systems
TRANSEC	Transmission Security
TRAP/TRE	TRE and Related Applications
TRE	Tactical Receive Equipment
UAV	Unmanned Aerial Vehicle
UHF	Ultra High Frequency